Before the
Federal Communications Commission

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunication	)	
Services	)	

Reply Comments of Lorrie Faith Cranor[1]

July 6, 2016

I would like to offer comments to address some of the questions the FCC's Privacy NPRM asks about robust authentication. I will focus on how authentication requirements may address the growing problem of mobile phone account hijacking and related fraud. I have conducted extensive research in the usable privacy and security area, and have co-authored over a dozen papers related to authentication and passwords with my colleagues and students at Carnegie Mellon University.[2] Recently I was a victim of mobile phone account hijacking, and have researched and written about this issue.[3]

Mobile phone account hijacking and SIM swap scams

Identity thieves are visiting mobile phone retail stores and impersonating account holders by showing fake drivers licenses or other falsified identity documents. Sometimes they are also asked to provide the last four digits of the victim's social security number. Typically they request to "upgrade" the mobile phones on the account, purchase new phones, or add new lines to the account. They claim that they do not have their phone with them because they forgot it, or that it has been lost or

[1] Lorrie Cranor, lorrie@cmu.edu. The author is submitting these comments as an individual. These opinions are her own.

[2] The CyLab Usable Privacy and Security Lab's password and authentication research papers are available at http://cups.cs.cmu.edu/passwords.html

[3] Lorrie Cranor. Your mobile phone account could be hijacked by an identity thief. Tech@FTC. June 7, 2016. https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief

broken. They receive new phones with the victim's phone numbers, and the phone equipment gets charged to the victim's account. The victim may discover something is wrong when their phone suddenly stops working because it has been transferred to the thief's new phone.

There appear to be two main motivations for this crime, with varying consequences for victims. One motivation is equipment theft: thieves obtain high-end mobile phones that they can resell on the black market. Another motivation is to gain access to the victim's phone number so that they can respond to text messages that are part of two-factor authentication schemes. Regardless of motivation, victims are inconvenienced by losing use of their mobile phone until their carrier restores their service, and by spending hours on the phone with their carrier or visiting their carrier's retail store to obtain new SIM cards, get their service restored, and have charges related to the theft refunded from their account. Some victims have found that their carriers act quickly to restore their service and refund charges, while others have found it difficult to convince their carrier that a theft has occurred. When a thief uses the victim's phone number to respond to two-factor authentication messages, the consequences for the victim can be much more severe – including significant financial losses, loss of control over their social network accounts,[4] and exposure of personal information contained in emails or stored in a breached account.

There are a number of variations on this scheme, which is referred to as mobile phone account hijacking, SIM swap, or SIM splitting. Instead of visiting a mobile phone store, some thieves perpetrate this crime by calling the victim's mobile carrier and ordering a new phone by mail, or requesting that their phone number be transferred to a new SIM card. In addition, instead of hijacking a victim's existing account, some thieves open up new accounts in a victim's name with a carrier that the victim has no existing account with.

In one variation of this attack, thieves first purchase the victim's bank account info or acquire it through a phishing attack. They may also look for publicly available information about the victim on social networks that can help them answer security questions. Then they impersonate the victim and call the victim's mobile phone company to report that their phone has been damaged or stolen and convince the company to cancel the SIM card and activate a new SIM card with the victim's phone number in the thieves' phone. The thieves are then able to make bank account transfers, responding to phone calls and text messages directed to the victim's phone number in order to complete the transactions. The victim's phone stops working as soon as the SIM card is swapped. It usually takes them several hours or

[4] Emily Dreyfuss. @Deray's twitter hack reminds us even two-factor isn't enough. Wired, June 10, 2016. https://www.wired.com/2016/06/deray-twitter-hack-2-factor-isnt-enough/

days to get their phone service restored, and longer to notice that their bank account has been emptied.[5]

Records of identity thefts reported to the FTC provide some insight into how often thieves hijack a mobile phone account or open a new mobile phone account in a victim's name. In January 2013, there were 1,038 incidents of these types of identity theft reported, representing 3.2% of all identity theft incidents reported to the FTC that month. By January 2016, that number had increased to 2,658 such incidents, representing 6.3% of all identity thefts reported to the FTC that month. Such thefts involved all four of the major mobile carriers. According to data from the Identity Theft Supplement to the 2014 National Crime Victimization Survey conducted by the U.S. Department of Justice, less than 1% of identity theft victims reported the theft to the FTC, so the FTC reports likely represent a very small fraction of a much larger problem.[6]

Robust authentication requirements

The Privacy NPRM asks about what authentication should be required "before granting a customer access to the customer's PI or before accepting another person as that customer's designee with a right to access a customer's PI."[7] Account changes such as moving a SIM card or phone number from one phone to another could result in granting someone purporting to be a customer or their designee access to a customer's personal information, and thus should be covered by authentication rules. To avoid ambiguity, I recommend that the FCC explicitly call out new account creation and changes to existing accounts as situations where robust authentication procedures are needed. In addition, account changes should be understood to broadly encompass changes to services, contact information, payment information, users, and devices[8] associated with an account.

The Privacy NPRM asks for input on robust authentication requirements, and few commenters have addressed this. Current authentication and credential verification

[5] Mary-Ann Russon. SIM swap fraud: The multi-million pound security issue that UK banks won't talk about. International Business Times, April 4, 2016. http://www.ibtimes.co.uk/sim-swap-fraud-multi-million-pound-security-issue-that-uk-banks-wont-talk-about-1553035

[6] See *supra* note 3

[7] Privacy NPRM ¶¶191-200

[8] Anecdotally, it appears that mobile carriers may not always consider mobile device changes as account changes, as customers seem to be able to obtain SIM cards with their phone numbers to put into new devices at carriers' authorized retail stores without authenticating themselves.

practices used by mobile carriers are insufficient to prevent account hijacking and related fraud. From my research, it appears that mobile carriers and retail stores that sell mobile phones on behalf of carriers generally require that account holders who come in person to request changes to their accounts authenticate with a photo identification card and sometimes the last four digits of a social security number. Some carriers will ask the account holder to provide a password established with the carrier under some circumstances. Without the use of verification tools, a photo identification card is not a sufficiently robust form of authentication for this purpose. Furthermore, the last four digits of a social security number are fairly easy to obtain and thus add little security. Depending on how the password is established and used, a password may or may not provide additional security, and may also lead to problems when account holders forget their password.

Due to changing technology and differences in the ways BIAS providers interact with their customers, I recommend allowing providers some flexibility in establishing authentication procedures informed by periodic risk assessments and updated to respond to the changing technology and security landscape. Such procedures should recognize that the risks to the subscriber associated with an unauthorized user making changes to their account may be substantial due to the widespread use of BIAS accounts as part of multi-factor authentication procedures for unrelated accounts.

Providers should periodically perform and document security risk assessments that identify attack vectors that have led to customer account compromise and that may lead to future customer account compromise. They should establish authentication procedures that are not unduly burdensome to their customers performing routine transactions, but that may require extra steps in higher-risk situations (for example when a mobile customer requests an account change but claims to have lost their phone).[9] Multi-factor authentication methods may or may not be necessary for routine transactions, depending on risk, but should always be offered to customers who want to use them (perhaps by allowing the customer to designate a multi-factor authentication provider to use, e.g. their email or social network provider). Authentication approaches may include a variety of factors such as appropriately-verified government-issued photo-IDs, one-time password verification codes, dynamic knowledge questions, passwords, biometrics, and other factors.

Government-issued photo-IDs are a convenient credential for most customers and have the potential to be reliable if used with appropriate verification procedures. Retail employees should be trained to properly verify these IDs and provided with verification tools, for examples tools that scan cards, perform optical character

[9] Other industries are starting to gain experience with such approaches, for instance to seamlessly authenticate mobile banking customers. A number of companies demonstrated authentication and credential verification solutions at the 2016 GSMA Mobile World Congress, for example.

recognition, and compare information printed on the card with information encoded in the card's barcode or send information to an ID verification service.

One-time password verification codes vary in their security and convenience. There are a variety of approaches to implementing them, for example through hardware tokens, mobile apps, and text messages, and new implementations are being introduced on a regular basis. It is important to assess both the usability and security of a particular implementation of one-time passwords for use in a specific context.

Many services require users to store answers to challenge or knowledge questions that can be used to recover their passwords. However, it is often easier for attackers to compromise accounts by obtaining the answers to these questions than by obtaining a user's password. This is due to the fact that knowledge questions that are easy for users to answer tend to rely on information that is easy to guess or learn from publicly available sources. Family members and friends often know the answers to typical questions such as mother's maiden name, name of your first pet, or city where you met your spouse. In addition, when users attempt to increase the security of their knowledge questions by giving false answers, they tend to provide false answers in predictable ways that can be guessed by attackers. Thus, experts recommend against the use of static knowledge questions as an authentication factor.[10] If knowledge questions are to be used as an authentication factor, it is advisable to use dynamically-generated questions (for example, drawn from a user's credit report or transaction records) rather than static questions with answers stored by the user in their account.

Currently, use of a security password is one of the only steps available to users to help prevent their mobile phone accounts from being hijacked, but it is not an ideal solution. Passwords used only for accessing personal information associated with a BIAS account can also be problematic, as users are unlikely to use these passwords frequently and thus are likely to forget them. It would be better for a BIAS provider to ask users to create a single password to authenticate them for all of their interactions with the provider (whether online, by phone, or in person), including logging into their online account, accessing personal information, and account changes. Such passwords should comply with current recommended password guidance.[11]

[10] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. 2015. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In Proceedings of the 24th International Conference on World Wide Web (WWW '15). ACM, New York, NY, USA, 141-150. DOI=http://dx.doi.org/10.1145/2736277.2741691

[11] NIST is in the process of updating their password recommendations. In May 2016 they posted "DRAFT NIST Special Publication 800-63B Digital Authentication Guideline" for comment at https://pages.nist.gov/800-63-3/

The Privacy NPRM also asks for feedback on the proposal to "notify customers of account changes, and attempted account changes, as an additional check against fraudulent account access."[12] This is a currently implemented best practice and makes sense to continue. Furthermore, as suggested above, providers should consider a broad definition of account changes when deciding when to notify customers. For example, a mobile phone customer should receive a notification when a retail store provides a new SIM card with their phone number. While there is a risk of overloading customers with too many account notifications, account changes do not typically occur on a regular basis. In addition, users should be able to access an archive of account changes and successful and failed attempts to access their account and personal information.

I recommend that for account changes that could enable an attacker to hijack an account (e.g. changing contact information, new users, new SIM cards, etc.), providers should go a step further and send a request for approval to the subscriber prior to the change. A back-up authentication system would be needed for cases where the device that the subscriber uses to receive these requests is lost or inoperable. To avoid exploitation, backup methods should be more difficult to compromise than the primary authentication method.

While robust authentication and notification procedures may reduce the incidence of account hijackings and related fraud, some fraud is likely to continue. The victims of such fraud are identity theft victims, and BIAS providers should establish processes for complying with Section 609(e) of the Fair Credit Reporting Act, which requires that companies provide business records related to identity theft to victims within 30 days of receiving a written request. Providers should disclose the process to their customers, including the address to which 609(e) requests should be sent.[13]

About the author

Dr. Lorrie Faith Cranor is a Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University where she is director of the CyLab Usable Privacy and Security Laboratory and co-director of the MSIT-Privacy Engineering masters program. In 2016 she is on leave from CMU while serving as Chief Technologist at the US Federal Trade Commission. She is also a co-founder of Wombat Security Technologies, an information security awareness training company. She has authored over 150 research papers on online privacy and usable

[12] Privacy NPRM ¶¶201-203

[13] https://www.ftc.gov/tips-advice/business-center/guidance/businesses-must-provide-victims-law-enforcement-transaction

security, and has played a central role in establishing the usable privacy and security research community, including founding the Symposium on Usable Privacy and Security. She was previously a researcher at AT&T Labs-Research. Cranor holds a doctorate in Engineering and Policy from Washington University in St. Louis. She is a Fellow of the ACM and IEEE. http://lorrie.cranor.org/

The author is submitting these comments as an individual. These opinions are her own.